REMARKS

In an office action dated September 08, 2004, informalities were cited in the specification and in various of the claims. Various of the claims were also objected to under 35 U.S.C. 112, second paragraph. The new set of claims should render moot the various objections for informalities and under 35 U.S.C. 112.

Rejection of Claims Under 35 U.S.C. 103(a)

Re: Lockhart (US 5,841,873) and Ahmed (US 6,747,961)

Re: Lockhart, Ahmed, and Latka (US 5,646,996)

Re: Lockhart and Menezes (Handbook of Applied Cryptography)

Lockhart is directed to a scheme of detecting cryptographic errors are generating reports thereof. Lockhart teaches the insertion of reference sequences into transmitted and encrypted data, and comparing such reference sequences to expected reference value at the receiver to determine cryptographic errors. However, Lockhart does not teach or envision the comparison of checksums for the purpose of detecting loss of stream-cipher synchronization. Lockhart specifically and explicitly teaches away from the notion that the payload checksums could be the reference value. The text at col. 5, lines 2-11 is exemplary of this point:

"However, one limitation on the reference value for the preferred embodiments, as will become clearer below, is that it must be determined and located prior to encryption of the appended data packet at step (209). Additionally any link or transport check sums such as a CRC should be added after the reference value and encryption of the data packet. The preferred implementation for appending the reference value (205) to the data packet is provided by appending a 2-byte fixed length field containing the ASCII characters "EN" after the last byte of the data packet."

A person applying Lockhart would invariably conclude that the reference value should be separate from the payload checksum. This is precisely opposite of the

motivation and thrust of the present claims, which are directed to reducing bandwidth while detecting loss of stream cipher synchronization. The very first lines of the Detailed Description of the present application make it clear that schemes such as those employed by Lockhart are inefficient and to be avoided:

"As discussed above, conventional communication systems employ inefficient encryption schemes that waste bandwidth to provide a mechanism to detect a loss of synchronization between encryption and decryption stream ciphers...Conventional systems require additional information to be transmitted with the encrypted payload, allowing a receiver to detect a loss of synchronization based on the additional information. Unfortunately, the additional information requires additional bandwidth." See specification of present application, Page 4, lines 1-9.

Lockhart would not anticipate the present claims, and there would be no motivation to apply Lockhart, precisely because it is one of the "conventional schemes...that waste bandwidth" and "require additional information to be transmitted with the encrypted payload."

The present claims further recite that the decryption occurs at a sub-network layer, whereas detection of loss of crypto synchronization occurs at a network layer. Nothing in Lockhart, Ahmed, or the other references teaches or suggests detecting the loss of cipher synchronization at a layer other than the layer that provides cryptography. These references also provide no motivation to provide decryption in one layer, and loss of synchronization in a higher layer, because they don't envision the synergy of using the network layer payload checksum to detect loss of synchronization. Instead, they rely on including additional crypto reference values in the stream, and so naturally would suggest detection of lost synchronization at the crypto layer where these reference values have meaning and are applied (the reference values have no meaning to the network layer).

For at least these reasons, the claims should be allowed over the cited prior art.

Thank you,

Charles A. (New) Mirho Reg. (New) 41,199

112 W. (New) 37th St., Vancouver, WA, 98660

Phone: 360-737-1748 Fax: 360-294-6426

Customer Number: 29586

Signature  Date 01-08-2005